APPEAL NO. 14-4658

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

v.

JOHN D. HAYES,

Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA AT HUNTINGTON

BRIEF OF APPELLANT JOHN D. HAYES

BRIAN J. KORNBRATH
ACTING FEDERAL PUBLIC DEFENDER

JONATHAN D. BYRNE
APPELLATE COUNSEL

DAVID R. BUNGARD
ASSISTANT FEDERAL PUBLIC DEFENDER

U. S. Courthouse, Room 3400
300 Virginia Street East
Charleston, West Virginia 25301
Telephone: 304/347-3350

Counsel for Appellant

Appeal No. 14-4658

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

v.

JOHN D. HAYES,

Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA
AT HUNTINGTON

BRIEF OF APPELLANT JOHN D. HAYES

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Federal Statutes

Other Authorities and Sources

STATEMENT OF JURISDICTION

On April 23, 2013, an indictment was filed in the Southern District of West Virginia charging John D. Hayes ("Hayes") with possession of child pornography, in violation of 18 U.S.C. §§2252A(a)(5)(B) and 2252A(b)(2). J.A. 12. After the district court rejected Hayes's guilty plea, the Government obtained a superseding indictment on December 18, 2013, charging Hayes with distribution of and attempt to distribute child pornography, in violation of 18 U.S.C. §§2252A(a)(2) and 2252A(b)(1) (Count One) and possession of child pornography (Count Two). J.A. 62. Because those charges constitute offenses against the United States, the district court had original jurisdiction pursuant to 18 U.S.C. §3231. This is an appeal from the final judgment and sentence imposed after Hayes was convicted on both counts following a bench trial. J.A. 677-680. A judgment order was entered on August 13, 2014. J.A. 754-760. Hayes timely filed a notice of appeal on August 19, 2014. J.A. 761. The United States Court of Appeals for the Fourth Circuit has jurisdiction pursuant to 18 U.S.C. §3742 and 28 U.S.C. §1291.

ISSUES FOR REVIEW

1. Whether Hayes provided a sufficient factual basis for a guilty plea to possession of child pornography, so that the district court should have accepted his guilty plea to the original one-count indictment.
2. Whether the use of evidence produced via an automated computer program to prove an essential element of the offense, introduced at

trial via a police officer who relied entirely on the program's results, violated Hayes's rights under the Confrontation Clause.

3. Whether evidence that Hayes maintained a file-sharing program on his computer that allegedly made child pornography available for download to others over the Internet is sufficient to support his conviction for attempted distribution of child pornography.

4. Whether Hayes's Sixth Amendment rights were violated by being sentenced to a mandatory minimum 15-year sentence for attempted distribution of child pornography based on prior convictions, without those convictions being alleged in the superseding indictment.[1]

STATEMENT OF CASE

This case began when a computer program informed law enforcement of a potential criminal offense involving child pornography. When Hayes attempted to plead guilty to possession of child pornography, the district court refused to accept that plea. The resulting trial, following a superseding indictment, saw Hayes convicted of both attempted distribution and possession of child pornography. The basis for the attempt conviction was the same computer

[1] Hayes recognizes that this issue is resolved by *Almendarez-Torres v. United States*, 523 U.S. 224 (1998), and *United States v. Cheek*, 415 F.3d 349 (4th Cir. 2005), which bind this Court. It is presented here to preserve it for further review.

program that had provided the initial tip. Hayes was sentenced to a mandatory minimum 15-year term of imprisonment as a result.

A. A police officer receives information that Hayes may be distributing or in possession of child pornography, based on a computer-generated tip.

Corporal Eddie Pritchard ("Pritchard") was the Huntington (West Virginia) contact for West Virginia's Internet Crimes Against Children Taskforce ("ICAC"), a group of officers who have been trained to investigate Internet-based crimes involving child pornography. J.A. 103-104. On May 1, 2012, Pritchard received a tip that files containing child pornography were available for download from a computer located in the Huntington area. The computer was identified by its Internet Protocol ("IP") address. J.A. 558, 560. The tip came from a nationwide computer database system called Child Protection System ("CPS"). J.A. 108.

CPS is "a tool for . . . authorized investigators" to obtain access to servers that store IP addresses of computers that were, at one time, offering files of child pornography for download over the Internet. J.A. 108-109, 558. It does so by monitoring the traffic of various peer-to-peer file sharing networks.[2] Once a suspect IP address is identified, CPS provides investigators with additional information about the content of the files it found and are available for download. J.A. 109. That information includes the name of the file, the SHA1 hash value for

[2] A peer-to-peer file sharing program allows computer users to share files with other users over the Internet. J.A. 229, 421-422.

each file,[3] and the Global Unique Identifier ("GUID") assigned to the particular version of the peer-to-peer software being used to offer the file. J.A. 112, 120, 224, 558, 560.

The CPS report Pritchard received identified an IP address (67.175.75.233) in the Huntington area that had reportedly made 16 child pornography image files available for download between March 17 and April 30, 2012. J.A. 560. He used that information to obtain an administrative subpoena from a local Internet provider, which identified Hayes as the subscriber linked to that IP address. Pritchard also obtained Hayes's address. J.A. 150.

With that information in hand, Pritchard procured a search warrant from a state court. J.A. 151. In the affidavit supporting his application, Pritchard stated he had observed a video file that CPS reported was available for download from Hayes's computer on April 11, 2012. J.A. 148-149, 560. His description included its file name,[4] hash number, and a detailed description of the video's contents. However, Pritchard never downloaded the file from Hayes's computer. Instead, he used the hash value to view another file with the same hash value that was

[3] A hash value is a mathematical algorithm of 40 characters which is a unique identifier of a particular computer file. J.A. 110, 420. It is frequently considered the equivalent of a fingerprint. *United States v. Wellman*, 663 F.3d 224, 226 n. 2 (4th Cir. 2011).

[4] The full filename was "(Hussyfan)(pthc)(r@ygold)Preteen Asian ALICIA, 11yo Philippine (Filipina) child prostitute XXX HC Pedo ptsc(2).mpg." J.A. 560.

stored as part of a collection of known child pornography files at the Huntington Police Department. J.A. 148-149.

B. Officers execute the search warrant at Hayes's home and take his statement.

On May 24, 2012, Pritchard and several other officers executed the search warrant at Hayes's home. J.A. 154, 630. They seized eight hard drives, 25 CD-ROMs, floppy disks, and one USB thumb drive.[5] J.A. 158, 631. While other officers were searching the home, Prichard advised Hayes of his *Miranda* rights, obtained a waiver of those rights, and took a statement from Hayes. J.A. 155-156, 180.

Pritchard asked Hayes about the kind of software he had on his computer and how he used it. Hayes explained that he had FrostWire, a peer-to-peer file sharing program. J.A. 161. He showed a basic awareness of how FrostWire worked and how to enter search terms to find and then download files from the Internet. Hayes said he used FrostWire to download music, TV shows, and movies. J.A. 180. When he downloaded files, he would move them to another folder on his computer. Sometimes, Hayes would preview the files as they were being downloaded. If he did not like the contents of the file, he would delete the file. Hayes told Pritchard he had been using FrostWire for two or three years. J.A. 163.

[5] That drive is also referred to in the record as a "flash drive."

Hayes told Pritchard that he had an interest in adult pornography and he hoped all of his downloaded material would be adult pornography. He explained that some of the video files he had downloaded had file names that did not match their actual content. As a result, Hayes did not know the content of any file until he actually viewed it. J.A. 181. Whenever Hayes downloaded a file that turned out to be child pornography, he deleted it. J.A. 181, 199. Hayes admitted that he had downloaded 30 to 40 images of child pornography over the past three or four months. J.A. 165. He also explained that he had downloaded files to the USB thumb drive, but he did not know what they were because he was unable to open the files to view them. J.A. 166.

C. Hayes is indicted for possession of child pornography. His attempt to plead guilty to that offense is rejected by the district court.

As a result of the evidence recovered at his home, Hayes was charged in a one-count indictment with possession of child pornography. Hayes filed a motion to schedule a guilty plea on October 24, 2013. J.A. 4. There was no written plea agreement with the Government. J.A. 18.

On November 5, 2013, Hayes appeared before the district court to enter a guilty plea. J.A. 14-32. After making certain that Hayes wished to enter a guilty plea, even without the benefit of a plea agreement, the district court asked Hayes to "[t]ell me in your own words what you did that makes you guilty." J.A. 20-21, 24. Hayes explained that he "was looking on the Internet for adult websites and I

came across – the wording of the files that I found were indicative of child porn, but some of them I had downloaded before had actually been adult." J.A. 24. The district court confirmed that Hayes had previously downloaded files with names suggestive of child pornography that actually turned out to be adult pornography. The district court confirmed with Hayes, "but you also saw some were children, minors." J.A. 25. Hayes went on to explain that "once I saw they were, you know, children, minors, I deleted those and kept the adult ones" because "I wasn't actually looking for the child; I was looking for adults. But the words and the wording of the name of the files were misleading." *Ibid.* He also confirmed that, with regard to the child pornography files found on the USB thumb drive, "I had actually downloaded those, but I'd never looked at them." J.A. 25-26. The district court summed up Hayes's statements:

> Q: And you would download what you thought was child pornography onto your computer or onto a flash drive. If you downloaded it and looked at it and saw it was child pornography, you said you immediately deleted it?
>
> A: Yes.
>
> Q: But there was some – there were some images on a flash drive that you had downloaded that you had not looked at.
>
> A: Right.

J.A. 26-27. Hayes discovered those images were child pornography "[w]hen the deputies came in." J.A. 27.

After this colloquy, the district court turned to defense counsel and said, "I don't see how the defendant has admitted the elements of the offense." J.A. 28. Counsel argued that Hayes had satisfied the knowledge requirement for possession of child pornography by admitting that he was aware that he had downloaded files with names suggestive of child pornography. Counsel distinguished between possession of child pornography, which required only the knowledge that the material is child pornography, with receipt, "because in receipt you have to have a knowing acceptance." *Ibid.*

The district court questioned Hayes further, and he explained that he used a program to search the Internet for "nudity" files, hoping to find adult pornography. J.A. 29-30. However, he agreed with the district court's description that "some of the sites or files . . . were labeled such that it – any person would assume that it was, in fact, child pornography?" J.A. 30. Hayes explained that a "file may say it was child pornography and it turned out to be adult, and the adult pornography would turn out to be child." *Ibid.* When asked if "at the time you decided to get the file, did you know and believe that it was probably going to be child pornography?" Hayes answered, "I took a chance that it wasn't." *Ibid.*

The district court concluded, "I don't think this gets it." J.A. 30. It further explained, "if the defendant is looking at sites for adult pornography and he says he finds sites that by their title might not have been adult, might have been children . . . he wasn't looking for child pornography and that he immediately

deleted anything he thought was child pornography." J.A. 30-31. The district court concluded the hearing without accepting Hayes's guilty plea. J.A. 32.

Hayes filed a motion urging the district court to reconsider its decision not to accept his guilty plea. J.A. 33-40. The Government filed a response stating that it "does not oppose the motion," but noting it was "considering filing additional charges against [Hayes] in the very near future." J.A. 50. The district court addressed that motion at a hearing on December 16, 2013. J.A. 53-70.

Hayes argued that courts (including this Court) had consistently rejected arguments that the child pornography statutes either included, or must include to avoid Constitutional infirmities, an element that a defendant intend to possess child pornography. J.A. 56. Hayes also argued that, based on his admission that he had downloaded child pornography in the past and then deleted it, that those files were still on the computer and, thus, still in his possession. J.A. 57. The district court disagreed and denied Hayes's motion. It concluded that, although Hayes found and downloaded child pornography files, "it wasn't because he was looking for child pornography; he was looking for adult pornography." J.A. 54. Therefore, "I just don't think that from what I heard at the plea hearing that the defendant has admitted a factual basis for guilt." *Ibid.* As to the possession of images that, while deleted were nonetheless still present on Hayes's computer, the district court concluded, "I still think the defendant denied any sort of intent that would be sufficient to establish guilt in a guilty plea proceeding." J.A. 55.

On December 18, 2013, the Government obtained the superseding indictment, charging Hayes with distribution of child pornography in addition to possession. J.A. 62-64. A bench trial on the two-count superseding indictment began on March 24, 2014. J.A. 86.

D. The Government presents evidence generated from a computer program as part of its case that Hayes was distributing child pornography.

Pritchard was the Government's first witness at trial. J.A. 102-201. He began by explaining how he had been trained, as part of joining the ICAC taskforce, to use CPS and about the kind of information it provided. J.A. 116. The Government used Pritchard to introduce a series of exhibits which contained CPS search results. One exhibit (Government Exhibit No. 4), was a screenshot taken by Pritchard from his computer monitor on May 1, 2012, showing the initial CPS report that there were child pornography files available from the IP address that matched Hayes's computer. J.A. 558. Pritchard testified that the exhibit showed that there were 16 "child notable" files being shared and available for download.[6] J.A. 560. It also showed that the search terms "pthc" and "10yo" had been entered by the use of the same IP address on April 19, 2012. J.A. 558. Pritchard explained that "pthc" stood for "preteen hard core," while "10yo" referred to the age of 10. J.A. 117. Later, one of the Government's forensic

[6] A "child notable" file is one that is "an image of a child in a sexually explicit manner," as compared with "child erotica," which is not covered by §2252A. J.A. 121-122.

experts would testify that there was no forensic evidence that Hayes had used those terms during Internet searches. J.A. 294-295.

Next, Pritchard explained the contents of Government Exhibit No. 5, a network activity report generated by CPS and printed in the form of a spreadsheet. J.A. 120-121. It listed all of the dates and times between March 17 and April 30, 2012 when a variety of files were reportedly available for download from Hayes's IP address. J.A. 560. The district court allowed Hayes to *voir dire* Pritchard about the exhibit and how it was generated, leading to his admissions that he was not responsible for the data it reflected and did not know how that data was collected. J.A. 123-128.

First, Pritchard explained that he did not use CPS on any of the dates between March 17 and April 30, 2012, to see what files, if any, were being shared by Hayes's IP address. J.A. 124. All of the information in the spreadsheet was generated as the result of a computer program with which Pritchard was not familiar. J.A. 136.

Second, Pritchard explained that one column on the spreadsheet, "Agent," showed the party who was responsible for each of the listings shown. All of the fields in this column were filled with "TLO." J.A. 125, 560. Pritchard testified that he knew TLO was a private corporation based in Florida that had developed the CPS software and was responsible for running the automated computer programs that searched shared folders on peer-to-peer networks. J.A. 126, 182.

TLO was also in the business of data mining, collecting information on individuals and selling it to various parties. J.A. 185. As to CPS, Pritchard explained that first "they [TLO] go out and check the shared folders of a particular computer at a particular IP address." J.A. 126. Next, "they compare the hash values of the files that are being shared . . . and they check them with the NCMEC[7] database to see if those hash values are – have been identified, and then it reports back what they have been identified as." *Ibid.* He testified that he did not know how TLO obtained the hash values, the descriptions provided for the files, or how TLO's search algorithms functioned. J.A. 186. In his opinion, TLO had automated a tedious process that Pritchard or other investigators would otherwise have had to do manually by downloading a suspect file from the IP address, comparing the hash values, and confirming whether the file matched one from the NCMEC database. It "basically made [it] easier for investigators" compared to "doing it old school." J.A. 126.

Third, Pritchard testified that the spreadsheet referenced computer programs Lime Scanner and Lime Crawler, both of which were used by TLO to run searches on peer-to-peer networks. J.A. 127, 183, 560. However, he did not use either piece of software himself and did not know how they worked. J.A. 127, 140, 184. Nor could he offer any opinion as to the reliability or accuracy of either

[7] NCMEC is the National Center for Missing and Exploited Children, which maintains a database of known child pornography files. See, *United States v. Richardson*, 607 F.3d 357, 360 (4th Cir. 2010).

program with regard to finding child pornography on peer-to-peer networks. J.A. 184.

Finally, Pritchard explained that there was another column on the spreadsheet, "Category," which purported to be a description of the listed file. J.A. 127, 560. He testified that he did not enter any of that information and assumed that CPS did it based upon the identified hash value. J.A. 127.

In light of Pritchard's admissions, Hayes objected to the introduction of Government Exhibit Nos. 4 and 5, and all the information contained in them, because they violated his right to confront witnesses against him. The information generated by CPS was generated only for law enforcement purposes and should be used only as a starting point for further investigation. J.A. 128-130, 135-136. The Government argued that the most of the information was computer generated, not the testimony of a witness, and therefore there was no witness to confront. J.A. 131. The exhibits were simply business records, admissible without need of confrontation. J.A. 134-135. Furthermore, the Government contended that it was not relying upon the "Category" column for proving its case. J.A. 134. Hayes responded that the entirety of Government Exhibit No. 5 was testimonial and being offered solely as evidence of the files that Hayes had allegedly made available for download. J.A. 135.

Upon further questioning from the district court, Pritchard explained that the TLO searches have been used by law enforcement for the past five years and

are considered reliable in cases like this one. J.A. 141. The district court delayed ruling on the confrontation objection. J.A. 141-142. However, during the examination of a later witness, the district court explained that "[t]hese are analytical tools recognized as reliable by people with training and experience" and "their admissibility is not really determined by the confrontation clause." J.A. 443-444 "Rather," the district court continued, "these are analytical tools used by people with technical expertise, and I believe that it's been properly authenticated, found to be reliable, and I deny the objection." J.A. 444.

Pritchard continued his testimony, during which the Government introduced Government Exhibit No. 5a, a condensed version of the earlier CPS spreadsheet. J.A. 561.[8] Pritchard identified a file on the spreadsheet that was allegedly available for download on April 11, 2012, at 4:26 a.m. from Hayes's IP address.[9] J.A. 148, 560 However, he had not attempted to download that file. Instead, he relied on the hash value from the spreadsheet and viewed a video file from the police media library that matched that value. J.A. 148. Pritchard did attempt to make connection with Hayes's IP address using peer-to-peer software at a later date, but was unsuccessful. J.A. 149.

[8] Hayes renewed his confrontation objection to this exhibit and the district court noted a continuing objection on that issue. J.A. 144.

[9] The full filename was "(Hussyfan)(pthc)(r@ygold)Preteen Asian ALICIA, 11yo Philippine (Filipina) child prostitute XXX HC Pedo ptsc(2).mpg." J.A. 560.

The Government subsequently introduced two others exhibits, Government Exhibit Nos. 4a and 5b, which related to CPS. J.A. 559, 562. The latter contained a list of files allegedly available for download from Hayes's IP address between March 17 and May 20, 2012. J.A. 562.

E. Multiple expert witnesses testify about the contents of the media seized from Hayes's home.

Following Pritchard, the Government called Christopher Vance ("Vance") of the West Virginia State Police. J.A. 203-331. Vance was a computer forensic expert and testified about the result of his examinations of various media recovered during the search of Hayes's home. J.A. 204. Vance participated in the search, seizing the USB thumb drive, labeled Removable Media 1 ("RM1"), from on top of a computer tower. J.A. 536, 565.[10] To examine RM1 and other media, Vance used a program that allows the users to locate files stored anywhere on a computer drive, including files that had been previously deleted by the user. J.A. 209-210. Using that program, Vance was able to locate 1441 deleted graphic files on RM1 and 3990 deleted files on one of the hard drives, "HD8." J.A. 289-90. Vance testified that Hayes did not have any type of forensic software on his computer that would have allowed him to view those deleted files. J.A. 288.

Vance also testified about the workings of the FrostWire peer-to-peer software that was found on another of the seized hard drives, "HD5." The

[10] Government Exhibit No. 10 contained copies of six files that were found on RM1.

software had been installed on November 16, 2011. J.A. 237, 573. The location designated by Hayes for downloading of files via FrostWire was a folder named "F\:\\Tattoos." J.A. 316-317, 573. Vance did not find a folder of that name on any of the seized hard drives or RM1. J.A. 234. He presumed that it was located on "HD6," a hard drive seized from Hayes's home that was not operable. J.A. 316-317. Vance also testified that the GUID value assigned to the version of FrostWire found on HD5 was the same as the GUID value reported by CPS. J.A. 235, 558. Based on the CPS report and the fact that the software showed an incoming connection had existed at some point, he concluded that "at one time sharing was enabled." J.A. 329. Finally, Vance admitted that Hayes could have downloaded the files on RM1 directly from the Internet without having to open and view them first. J.A. 283.

Hayes presented testimony from his own forensic expert, Michael Maschke ("Maschke").[11] J.A. 332-399. Maschke found an earlier installation of FrostWire (on a drive designated "HD7"), which had been installed and last used on October 15, 2010. J.A. 336-337, 645-647. The version of FrostWire found on HD5, Maschke testified, had been last used on May 20, 2012. J.A. 338, 648-650. At the time the search was executed, the sharing function on that version of

[11] Maschke testified out of order, during what was otherwise the Government's case in chief. J.A. 330-331.

FrostWire had been turned off. J.A. 338-339, 648-650.[12] If the sharing function was turned off, there would be no way for another person to download any files over the Internet. J.A. 616-620

Maschke also testified that he found numerous folders with names suggestive of pornography that were created and deleted on the same day. J.A. 343-345, 644. In addition, he explained that there were only 18 files on RM1 that contained child pornography and could have been accessed by Hayes. J.A. 348, 644. An additional 18 files on RM1 had been deleted within a couple of days of the date they were created. J.A. 348-349, 397.

Maschke further testified about the file tree listings from Hayes's hard drives that showed the location of user-created folders and files. J.A. 351, 651-676. He explained that Hayes appeared to possess numerous folders of non-pornographic television shows and movies downloaded from the Internet. J.A. 359-361, 657, 659, 661, 662. He also found evidence that Hayes made some downloads using Torrent, another peer-to-peer program, in which the person who offers a file for upload is responsible for naming it. J.A. 357-358, 658-660. As a result, there is no way of knowing the contents of a file until it has been downloaded and viewed by the end user. J.A. 359, 385.

[12] Maschke also explained that the sharing function has been turned on at some point in the past. J.A. 370.

F. The district court finds Hayes guilty on both counts of the superseding indictment.

Following the close of evidence and arguments by the parties, the district court found that Hayes was guilty of "attempt to distribute child pornography" and "possession of child pornography," as charged in the superseding indictment. J.A. 524-525.[13] As to possession, the district court found that "the circumstantial evidence as to the defendant's intent to possess child pornography is, in fact, overwhelming." J.A. 525. As to attempted distribution, the district court found that Hayes was "sophisticated enough" a computer user to "understand what FrostWire was used for" and that it could only provide access to its shared files at his request. J.A. 529-530. Although the file-sharing portion of FrostWire was turned off when HD5 was seized, the district court found "reliable and persuasive the evidence from the CPS program that on dates prior to that . . . the sharing capability was enabled" and that "the CPS software was able to identify files on the defendant's storage devices that were available for sharing and which were also child pornography." J.A. 530. And while "there's simply insufficient evidence to show that a transfer actually took place," Hayes's use of FrostWire "and his decision to possess and keep and make available child pornography" showed that he "intended that other people would be able to access his stored child pornography and download it if they so desire." J.A. 531. In a written order

[13] The district court had earlier denied Hayes's motion for a judgment of acquittal. J.A. 480-491.

memorializing the verdict, the district court stressed the importance of CPS to its verdict, noting that it "found the defendant had files available to share with hash values previously identified as child pornography" and the "program could not have discovered those hash values unless the defendant had enabled the sharing capabilities of FrostWire . . .." J.A. 679.

G. Hayes is sentenced to 15 years in prison.

Following Hayes's conviction, a Presentence Investigation Report ("PSR") was prepared to assist the district court at sentencing. J.A. 782-807. The probation officer recommended that Hayes's advisory Guideline "range" was life in prison. J.A. 798. As relevant to this appeal, the probation officer also identified the statutory sentencing ranges as being 15 to 40 years in prison on Count One and 10 to 20 years in prison on Count Two. J.A. 797.

The statutory mandatory minimum sentences on both counts applied because of Hayes's 1979 convictions for Second Degree Sexual Assault. 18 U.S.C. §2252A(b)(1) and 2252A(b)(2); J.A. 538-540, 793. Prior to sentencing, Hayes objected to the enhanced sentences, arguing that the prior convictions were not charged in the indictment. J.A. 684-685, 713, 714, 806. The district court overruled Hayes's objection, based on binding Supreme Court precedent. J.A. 714. It then sentenced Hayes to the mandatory minimum 15 years in prison. J.A. 743, 756.

SUMMARY OF ARGUMENT

Hayes's conviction for attempting to distribute child pornography must be vacated, for each of several reasons. First, that offense was only charged in a superseding indictment because the district court erroneously concluded that Hayes had not laid a sufficient factual basis for pleading guilty to possession of child pornography. Had the district court correctly accepted Hayes's guilty plea to possession, there would have been no distribution or attempted distribution charged by the Government. Second, the key evidence against Hayes on the attempted distribution charge came in the form of reports generated by a computer program. The Government witness who presented those reports did not know how the program worked, nor were any other witnesses presented through which Hayes could challenge the program's reliability. The inability to do so denied Hayes his right to confront witnesses against him. Finally, the evidence presented at trial was insufficient to prove that the Hayes attempted to distribute child pornography.

ARGUMENTS

I. Hayes provided a sufficient factual basis for a plea of guilty to possession of child pornography. The district court erred by rejecting his guilty plea and subjecting him to trial on the superseding indictment.

A. Standard of Review

In considering a defendant's guilty plea, a district court "possesses wide discretion in determining whether a sufficient factual basis exists" and this Court reviews the district court's decision for abuse of discretion. *United States v. Mitchell*, 104 F.3d 649, 652 (4th Cir. 1997). However, a district court "necessarily abuses its discretion when it makes an error of law." *Sloas v. CSX Transp., Inc.*, 616 F.3d 380, 388 (4th Cir. 2010); *Nelson-Salabes, Inc. v. Morningside Development, LLC*, 284 F.3d 505, 512 (4th Cir. 2002)("when we review the legal conclusions of a district court, we do so on a *de novo* basis").

B. Hayes's admissions at the guilty plea hearing were sufficient to provide a factual basis that he was guilty of the crime of possession of child pornography.

Hayes was originally charged only with possession of child pornography. He attempted to plead guilty to that offense, explaining to the district court how he downloaded child pornography while searching for adult pornography. The district court found Hayes did not provide a sufficient factual basis because he did not admit to seeking out child pornography, importing an intent element into the offense of possession of child pornography that this Court and others have

rejected. The district court's error had profound impact on Hayes and led to his mandatory minimum 15-year sentence.

C. A district court must accept a defendant's guilty plea if certain grounds are met.

The Rules of Criminal Procedure present a defendant charged with a crime three options with regards to a plea – he "may plead not guilty, guilty, or (with the court's consent) nolo contendere." Federal Rule of Criminal Procedure 11(a)(1). A guilty plea is "an admission of all the elements of a formal criminal charge." *United States v. Mancinas-Flores*, 588 F.3d 677, 681 (9th Cir. 2009), citing *McCarthy v. United States*, 394 U.S. 459, 466 (1969). Notably, only the nolo contendere plea or a conditional guilty plea are predicated on being entered with the consent of the court. *Id.* at 11(a)(3). Thus, "it is clear that a court must accept an unconditional guilty plea, so long as the Rule 11(b) requirements are met." *In re Vasquez-Ramirez*, 443 F.3d 692, 695-696 (9th Cir. 2005).

One of those requirements is that "[b]efore entering judgment on a guilty plea, the court must determine whether there is a factual basis for the plea." Federal Rule of Criminal Procedure 11(b)(3). The requirement of determining the factual basis for a guilty plea allows "the court [to] make clear exactly what a defendant admits to, and whether those admissions are factually sufficient to constitute the alleged crime." *United States v. DeFusco*, 949 F.2d 114, 120 (4th Cir. 1991). It "is designed to 'protect a defendant who is in the position of pleading

voluntarily with an understanding of the nature of the charge but without realizing that his conduct does not actually fall within the charge.'" *United States v. Mastrapa*, 509 F.3d 652, 660 (4th Cir. 2007), quoting Federal Rule of Criminal Procedure 11, Advisory Committee Notes (1966). To determine whether a factual basis exists for the guilty plea, the district court may look to "anything that appears on the record," not just the plea colloquy itself. *Id.* at 660. A district court may even find a factual basis exists for a guilty plea when the defendant maintains his innocence. See, *North Carolina v. Alford*, 400 U.S. 25 (1970).

At the guilty plea hearing, the district court asked Hayes to explain "in your own words what you did that makes you guilty." J.A. 24. Hayes explained that he was looking for adult pornography, but that he downloaded files with names suggestive of child pornography and downloaded files that appeared to contain child pornography. He deleted files that appeared to involve minors. J.A. 25. As he told the district court, a "file may say it was child pornography and it turned out to be adult, and the adult pornography would turn out to be child." J.A. 30. Hayes "took a chance" that files with names suggestive of child pornography would contain adult pornography instead. *Ibid.*

The district court concluded that, as a factual basis, "I don't think this gets it" because "he wasn't looking for child pornography and . . . he immediately deleted anything he thought was child pornography." J.A. 30-31. In denying Hayes's motion to reconsider, the district court was clear that the fact that Hayes

possessed child pornography files was not sufficient because "it wasn't because he was looking for child pornography; he was looking for adult pornography." J.A. 54. Furthermore, the district court concluded that "I still think the defendant denied any sort of intent that would be sufficient to establish guilt in a guilty plea proceeding." J.A. 55.

Numerous courts, including this one, have concluded that child pornography offenses under §2252 and §2252A do not have, nor are required to have, an element of intent to them. It is enough for a person to have possession of the images and know of their character. The district court's erroneous legal application of an intent requirement upon Hayes conflicts with those cases.

D. A person who downloads what he knows or should know is child pornography is guilty of possession of child pornography, even if he was not acting with any ill intent when doing so.

This Court addressed the issue of intent in child pornography offenses in *United States v. Mathews*, 209 F.3d 338 (4th Cir. 2000), relying heavily on the Supreme Court's decision in *United States v. X-Citement Video, Inc.*, 513 U.S. 64 (1994). Mathews was an investigative journalist who had produced a three-part radio series on child pornography and its prevalence on the Internet. *Mathews*, 209 F.3d. at 339. Once the series ran, Mathews continued his research, which included "initiat[ing] conversations with individuals who identified themselves as minor females, and engag[ing] them in sexually explicit discussions." *Id.* at 340.

Many of those minors, however, were undercover FBI agents who documented Mathews sending or receiving "160 photographs depicting child pornography." *Ibid.* He was charged with multiple counts of sending and receiving child pornography under 18 U.S.C. §2252. *Ibid.*

Mathews moved to dismiss the charges, arguing that §2252 "was unconstitutional as applied to him, a bona fide journalist researching a news story" because it violated the First Amendment. *Mathews*, 209 F.3d at 341. He also argued that the statute "violated his due process rights because it contained no *mens rea* element requiring a person transmitting child pornography to 'have a morally blameworthy mental state when doing so.'" *Ibid.* The district court denied the motion, and Mathews entered a conditional guilty plea. *Id.* at 341.

After rejecting the First Amendment argument, this Court turned to Mathews's argument "that if §2252 is interpreted to require only receipt or transmission of images known to be child pornography, the statute violates the Due Process Clause 'because it contains no criminal intent requirement, even though nothing suggests Congress desired such a harsh result.'" *Mathews*, 209 F.3d at 350. Per Mathews, reading §2252 without an intent requirement "poses a constitutional problem" that was particularly evident "in light of the possibility that an Internet user could innocently view child pornography." *Ibid.* This Court disagreed, noting that "Congress settled on 'knowingly' as the required mental state" when drafting the statute and the "plain language of the statute requires

nothing more." *Id.* at 351. "Nor," this Court concluded, "does the Constitution mandate that the statute be interpreted to require proof that a defendant acted with a bad motive or evil intent" such as "to satisfy some prurient interest." *Ibid.* Thus, "Mathews's admission that he knew he was receiving and transmitting child pornography is all that was required to prove that his conduct was knowingly carried out." *Id.* at 352 (internal quotation omitted).

The Eleventh Circuit faced an issue similar to Hayes's in *United States v. Alfaro-Moncada*, 607 F.3d 720 (11th Cir. 2010). Alfaro-Moncada was found guilty of possession of child pornography based on several DVDs found on the ship where he worked. In affirming the sufficiency of the evidence, the court rejected Alfaro-Moncada's argument that he did not intend to purchase child pornography and did not know of the DVDs' contents until after he purchased them. Calling the argument "free of anything resembling merit," the court noted that Alfaro-Moncada testified that he "had looked at the covers of the DVD cases . . . and watched a 'little bit' of the DVDs inside. At that point, by his own admission, he knew that he was in possession of child pornography." *Id.* at 733. His intent to throw them overboard after he learned that was irrelevant.

In addition to decisions like *Mathews* and *Alfaro-Moncada* that make it clear that no ill intent is needed to sustain a conviction involving child pornography, other courts have held that the knowledge requirement in the statute is easily met. In *United States v. Haymond*, 672 F.3d 948, 957 (10th Cir. 2012), the court rejected

the defendant's argument that he was unaware of the contents of the images at issue where he "used search terms associated with child pornography to find and the downloaded the charged images" using peer-to-peer software. In *United States v. Irving*, 452 F.3d 110, 122 (2nd Cir. 2006), the court held that a defendant's knowing possession could be proven based on the fact that images were found on his computer and there was "no showing that someone else lived at his apartment, or had access to his computer." See also, *United States v. Rogers*, 714 F.3d 82, 86 (1st Cir. 2013); *United States v. Miller*, 527 F.3d 54, 62-64 (3rd Cir. 2008). Courts have also held that deleted images or images stored in an Internet cache have been "knowingly" possessed. See, *United States v. Romm*, 455 F.3d 990, 998-1001 (9th Cir. 2006).

The child pornography statutes provide separate offenses for knowing receipt of child pornography, versus mere possession. 18 U.S.C. §2252(a)(2). In cases examining the elements of the receipt charge, courts have emphasized the low burden required to sustain a possession conviction. As the Seventh Circuit explained, "a person who seeks out only adult pornography, but without his knowledge is sent a mix of adult and child pornography, will not have violated" the receipt provision. *United States v. Myers*, 355 F.3d 1040, 1042 (7th Cir. 1040). However, "[t]hat same person . . . could be in violation of the possession provision of §2252(a)(4)(B) if he or she decides to retain that material, thereby knowingly possessing it." *Ibid.* The distinction in *Myers* captures Hayes's admitted

conduct accurately – he wanted to receive adult pornography, but received both adult and child pornography from the Internet and decided to retain, at least for some amount of time, the child pornography. That is doubly true because even the deleted files were still available to Hayes and therefore possessed by him. Hayes provided a sufficient factual basis for the entry of a guilty plea to the offense of possession of child pornography. The district court erred by concluding otherwise. See, *Leak v. United States*, 2011 WL 2971967, *5 (N.D.W.Va. 2011)(defendant's admission at guilty plea hearing that "child pornography existed on his work computer, that he viewed it, and that he subsequently attempted to delete it from his computer's hard drive . . . provides a sufficient basis to support his guilty plea").

E. The district court's erroneous decision that Hayes had not laid a sufficient basis to enter a guilty plea greatly prejudiced Hayes.

The district court's erroneous rejection of Hayes's guilty plea had a profound effect on the outcome of his case. Had the district court accepted Hayes's guilty plea he would have been subject to a term of imprisonment of between 10 and 20 years in prison.[14] After the rejection of Hayes's guilty plea, the Government obtained a superseding indictment, alleging (in addition to the possession count) that Hayes distributed child pornography as well. J.A. 62-64.

[14] Although, as argued on pages 46 to 49 below, under current Sixth Amendment doctrine, the range should only be zero to 10 years.

After Hayes was eventually convicted at trial of attempting to distribute child pornography, his mandatory minimum sentence increased to 15 years in prison and his statutory maximum to 40 years in prison. Given the district court's imposition of that mandatory minimum sentence, it is likely that had Hayes's initial guilty plea been accepted, he would have received a 10-year, rather than 15-year, sentence.

Moreover, the rationale given for finding Hayes guilty on the possession charge during Hayes's bench trial did not follow from that used to reject Hayes's guilty plea. Initially, the district court continued to err by focusing on Hayes's intent, concluding that "the circumstantial evidence as to the defendant's intent to possess child pornography is, in fact, overwhelming." JA. 525. Later, in setting forth that evidence, the district court noted that the images Hayes was downloading "by the title . . . [i]t is relatively clear that any person accessing or seeking this type of file material is looking for and going to obtain child pornography." J.A. 527. Furthermore, Hayes's deletion of many of the files "only underscores the defendant's knowledge and understanding of how to use his computer skills . . . to avoid detection or prosecution for possessing child pornography." *Ibid.* None of the actions taken by Hayes are any different than the actions he admitted taking during the guilty plea. The only difference is Hayes's intent, which, as shown above, is irrelevant to his guilt.

In light of the district court's error and the prejudicial impact upon Hayes, this Court must vacate the district court's decision rejecting Hayes's guilty plea, vacate his conviction for attempted distribution of child pornography, and remand his case for resentencing on a single count of possession of child pornography.

II. The use of evidence generated by CPS, a computer program, to convict Hayes for attempted distribution of child pornography violates his right to confront all witnesses against him under the Sixth Amendment.

A. Standard of Review

This Court reviews "alleged Confrontation Clause violations under the *de novo* standard of review." *United States v. Lighty*, 616 F.3d 321, 376 (4th Cir.2010)

B. Hayes was denied the right to confront the most important witness against him, violating his rights under the Sixth Amendment.

The Sixth Amendment provides that "the accused shall enjoy the right . . . to be confronted with the witnesses against him." For decades, the Supreme Court's confrontation jurisprudence looked only to the reliability of proffered evidence. See, *Ohio v. Roberts*, 448 U.S. 56 (1980). More recently, however, the Court has returned the analysis to the means of reliability testing provided by the Sixth Amendment itself – confrontation. *Crawford v. Washington*, 541 U.S. 36, 62 (2004)("Dispensing with confrontation because testimony is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty. This is

not what the Sixth Amendment prescribes"). Thus, "[t]estimonial statements of witnesses absent from trial" are not admissible, unless the defendant has had a prior opportunity to cross examine that witness. *Id.* at 59. More recently, the Court has extended that holding to scientific and expert testimony. See, *Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009); *Bullcoming v. New Mexico*, ___ U.S. ___, 131 S.Ct. 2705 (2011). With regard to Hayes's conviction for attempted distribution of child pornography, the most important witness(es) against him were the unknown programmers at TLO who developed the CPS software upon which law enforcement relied entirely to conclude that Hayes had made child pornography available for distribution. The entry of that testimony into evidence violated Hayes's right to confront the witnesses against him.

C. The only evidence that Hayes made child pornography files available to others over the Internet came from a computer program created by a private company about which the Government's witnesses knew little.

None of the child pornography files allegedly made available by Hayes were ever downloaded, either by other users or law enforcement. Nor did any human being ever see, on his or her computer screen, the files available for download. The only evidence of such files being offered came from CPS, a computer program about which the Government's witnesses knew very little. Pritchard knew that it was "a tool for . . . authorized investigators" of child pornography and that it monitored traffic over peer-to-peer networks. J.A. 108-109. He knew

that CPS was a product produced by a private company in Florida, TLO, although he did not know what "TLO" stood for. J.A. 1215, 126.[15] He did not know how the program or TLO obtained information about the files it found or how the search algorithms functioned. J.A. 186. He was not familiar with either piece of software that TLO used to find files on peer-to-peer networks and, as such, could not offer any opinion as to their reliability or accuracy of finding child pornography. JA. 127, 140, 184. For example, he could not explain why one of the files, reported as child pornography but actually a music file, by CPS was titled "Herman Hermits - Mrs. Brown you've got a lovely daughter - 1965.avi." J.A. 188-189.[16] Nor was there an explanation as to why CPS reported that terms associated with child pornography, such as "pthc" or "10yo," had been entered from Hayes's IP address, while the Government's own expert witness found no forensic evidence that Hayes ever used those terms. J.A. 294-295, 558. What Pritchard did know is that CPS "basically made [it] easier for investigators" in such cases compared to "doing it old school." J.A. 126. That is, compared to the

[15] It is not clear that "TLO" actually stands for anything at all. See, http://www.tlo.com/ (last visited November 4, 2014), website of the company now known as "TransUnion TLO."

[16] "Mrs. Brown, You've Got a Lovely Daughter" was a number one hit for Herman's Hermits in 1965. http://en.wikipedia.org/wiki/Mrs._Brown,_You've_Got_a_Lovely_Daughter (last visited November 4, 2014). CPS also identified files from popular artists such as Kelly Clarkson, The Beatles, and Bob Seger as being available. J.A. 562.

investigators themselves actually compiling allegedly incriminating evidence directly from a suspect's computer.

The CPS program was the Government's most crucial fact witness at trial. The reports it produced were the only evidence that Hayes had made child pornography files available for download on the Internet. It provided the file names, the hash values, and a description of their alleged content. J.A. 560-562. Without that evidence, the Government would have had no case against Hayes. The district court's rulings finding him guilty of attempted distribution of child pornography demonstrate that. When finding that Hayes had enabled the file-sharing capability of FrostWire, it was based on "reliable and persuasive . . . evidence from the CPS program that . . . the sharing capability was enabled." J.A. 530. Furthermore, it relied on the fact that "the CPS software was able to identify files on the defendant's storage devices that were available for sharing and which were also child pornography." *Ibid.* In its written order, the district court noted that it was CPS that "found the defendant had files available to share with hash values previously identified as child pornography." J.A. 679. It also noted that the "program could not have discovered those hash values unless the defendant had enabled the sharing capabilities of FrostWire . . .." *Ibid.* Thus, Hayes was convicted on the testimony of a witness he never confronted.

D. Documents kept in the usual course of business, if they are produced for use at trial, are not exempt from the requirements of confrontation. Nor should the fact that the statements were the result of a computer program change the analysis.

The First Circuit faced a similar issue in *United States v. Cameron*, 699 F.3d 621 (1st Cir. 2012), also a child pornography prosecution. Cameron was convicted after a trial at which the district court admitted records from Yahoo! and Google regarding his activities. On appeal, the court grappled with Cameron's argument that the admission of those documents violated his right to confront witnesses against him. The court agreed as to some of the documents and reversed Cameron's convictions. *Id.* at 626.

Primary among the issues confronted by the court in *Cameron* was whether the documents at issue were business records. *Cameron*, 699 F.3d at 639. The Government made the same argument as it did in this case with regard to the CPS documents – that they were business records not subject to confrontation. J.A. 134-135. However, as the *Cameron* court noted, although the Supreme Court initially proclaimed in *Crawford* that "business records are not testimonial 'by their nature,' the Court later indicated that this is not necessarily the case for all business records." *Cameron*, 699 F.3d at 639, quoting *Crawford*, 541 U.S. at 56. The Supreme Court went on to note "that although '[d]ocuments kept in the regular course of business may ordinarily be admitted at trial despite their hearsay status,' this would not be so 'if the regularly conducted business activity is the

production of evidence for use at trial.'" *Id.* at 640, quoting *Melendez-Diaz*, 557 U.S. at 321; see also, *Bullcoming*, 131 S.Ct. at 2720.

Turning to the evidence, the court first concluded that the admission of documents produced by Yahoo!'s account management tool and login tracker and Google Hello's connection logs did not violate Cameron's right to confrontation because they were full of data "automatically collected in order to further its business purposes." *Cameron*, 699 F.3d at 641. As a result, they were not testimonial and not subject to confrontation. *Id.* at 641-642. By contrast, the court found that the child pornography reports prepared by Yahoo!, and the subsequent NCMEC CyberTipline reports that simply passed them on, were subject to confrontation. *Id.* at 642-652. It concluded that the statements were made out of court by a person (a Yahoo! employee) and offered for the truth of the matter asserted. *Id.* at 642. On the last prong, the court concluded that "we can only infer that it was the government's intent to use this evidence to link Cameron to the specific IP addresses from which child pornography images were *uploaded* into the Yahoo! accounts . . .." *Id.* at 642-643. Although such records were kept in the regular course of Yahoo!'s business, "there is strong evidence" that they "were prepared with the 'primary purpose of establishing or proving past events potentially relevant to a later criminal prosecution.'" *Id.* at 643, quoting *Bullcoming*, 131 S.Ct. 2714, fn. 6.

The CPS reports are similar to the child pornography reports found to be testimonial statements in *Cameron*. They were made out of court and, like the Yahoo! reports, although they were produced in the regular course of business, "the regularly conducted business activity is the production of evidence for use at trial." *Melendez-Diaz*, 557 U.S. at 321, citing *Palmer v. Hoffman*, 318 U.S. 109, 114 (1943)(business record inadmissible where it was "calculated for use essentially in the court, not in the business"). That is doubly so for the CPS reports, as TLO is in the business of providing such documents to authorities for use in criminal investigations. J.A. 108-109; *TLO Files for Chapter 11 Reorganization to Facilitate Financial Restructuring*, May 9, 2013 (during reorganization "we will continue to provide TLO's Child Protection System to law enforcement in more than 40 countries around the world to identify and locate child predators").[17] Furthermore, the CPS reports played a crucial role in the district court's conclusion that Hayes was guilty of attempting to distribute child pornography. Contrary to the Government's contention that the data only "served as a jumping off point to start the investigation," J.A. 8, Docket No. 93, at 9, it was actually the Government's star witness at trial.

No other court has approved of the use of CPS as it was employed in this case. In most cases where CPS is mentioned, it was used as the investigative tool

[17] Available online at http://www.tlo.com/news.html?id=7 (last visited November 4, 2014).

Pritchard testified that it is – as a "jumping off point," and nothing more. See, e.g., *United States v. Dodson*, 960 F.Supp.2d 689 (W.D. Tex. 2013)(use of CPS did not constitute an illegal warrantless search); *United States v. Dennis*, 2014 WL 1908734 (N.D. Ga. 2014)(same). The unpublished Fifth Circuit case upon which the Government relied below does not suggest a broader role. *United States v. Larman*, 547 Fed.Appx. 475 (5th Cir. 2013); J.A. 8, Docket No. 93, at 8. Although Larman raised a sufficiency of the evidence claim, he did not challenge the validity of the CPS evidence offered. Instead, he argued that the CPS data could not prove that someone else with access to the computer could have downloaded the child pornography at issue. *Id.* at **5.

The only distinction between the CPS reports and the Yahoo! reports in *Cameron* is that the Yahoo! reports were produced directly by a human being. By contrast, the CPS reports are produced by a computer program. That is a distinction that should not make a difference. Reports like the one generated by CPS do not appear out of thin air. They are the result of countless human inputs, decisions, and judgment calls – none of which the Government's witness knew anything about. Computer programs do not write themselves. The machines that run them are not (yet) sentient. Thus, when Pritchard agreed that the "Category" field in the CPS report was "something that the program does based on information it already has," he is actually saying that the results are based on previously programmed human inputs. J.A. 121. Similarly, when he testified that

he was "assuming the program" entered the file descriptors "based on the hash value," he was referring to the human inputs that created those outputs. J.A. 127.

This Court's decision in *United States v. Washington*, 498 F.3d 225 (4th Cir. 2007), does not require the adoption of a simple dichotomy between human and non-human testimony. In *Washington*, the defendant challenged the Government's failure to introduce the raw data upon which its expert witness testified that the defendant was under the influence of PCP while driving. *Id.* at 227. That data consisted of "mechanical computer printouts" generated by a gas chromatograph. *Id.* at 228. After concluding that the "statements" at issue were not those of the technicians who operated the machine but of the machine itself, this Court noted that statements "made by machines are not out-of-court statements made by declarants that are subject to the Confrontation Clause." *Id.* at 230. Thus, "no out-of-court statement implicating the Confrontation Clause was admitted into evidence through the testimony of" the Government's expert witness. *Id.* at 231. Unlike *Washington*, the mechanical statements in this case did not consist merely of raw data later interpreted by an expert who was subject to cross-examination at trial. Instead, they were fact statements reporting the presence of particular files available at Hayes's IP address on a particular date. The mechanical statements in *Washington* provided the raw data that the defendant was under the influence, they did not provide direct testimony as evidence of his intoxication.

E. Hayes's conviction for attempted distribution of child pornography must be reversed because he was unable to cross-examine the key witness against him.

Computers do only what humans tell them to do, hence the well-known programmer aphorism, "Garbage In, Garbage Out." See, *Wohl v. Spectrum Mfg.*, 94 F.3d 353, 355 (7th Cir. 1996); *United States v. Esquivel-Rios*, 725 F.3d 1231, 1234 (10th Cir. 2013)("Everyone knows that much about computers: you give them bad data, they give you bad results"). Nonetheless, computers have a "mystifying quality" and "an aura of reliability that may be unwarranted, but nevertheless hard to dispel." Robert Garcia, *"Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution*, 38 UCLA L. Rev. 1043, 1049 (1991). This has led to a revised aphorism – "Garbage In, Gospel Out ." *Id.* at 1049, fn. 18 ("[a]ccording to Pierre Galois, 'If you put tomfoolery into a computer, nothing comes out but tomfoolery. But this tomfoolery, having passed through a very expensive machine, is somehow ennobled and no one dares criticize it'").

That "mystifying quality" of computer-generated evidence is evident in this case. No witness testified as to how CPS actually worked, the parameters it used in its searches, or how accurate its results are. That is particularly critical in this case because no one – not investigators, not other users – was shown to have actually downloaded the files CPS said Hayes made available for download by others. Nevertheless, the district court found CPS to be a "reliable and persuasive" witness that "was able to identify files" available for download. J.A.

350. The Government's case as to attempted distribution rise and fell on whether the CPS reports were accurate. Hayes was denied his opportunity to determine their accuracy in the only mechanism provided by the Constitution – cross examination of the witness against him. The introduction of those reports was error that requires the reversal of Hayes's conviction for attempted distribution of child pornography.

III. Evidence that Hayes maintained a peer-to-peer file sharing program and made files available to others over the Internet is not sufficient to convict Hayes of attempting to distribute child pornography.

A. Standard of Review

"In assessing the sufficiency of the evidence presented in a bench trial, we must uphold a guilty verdict if, taking the view most favorable to the Government, there is substantial evidence to support the verdict." *Elliott v. United States*, 332 F.3d 753, 760-61 (4th Cir. 2003). "[S]ubstantial evidence is evidence that a reasonable finder of fact could accept as adequate and sufficient to support a conclusion of a defendant's guilt beyond a reasonable doubt." *United States v. Burgos*, 94 F.3d 849, 862 (4th Cir. 1996)(*en banc*).

B. There was insufficient evidence to show Hayes attempted to distribute child pornography.

In the superseding indictment, Hayes was charged with both distribution and attempted distribution of child pornography. J.A. 62-64. The district court convicted only on attempted distribution, noting that "there's simply insufficient

evidence to show that a transfer [of child pornography to someone else] actually took place." J.A. 531. However, Hayes's use of the FrostWire peer-to-peer software "and his decision to possess and keep and make available child pornography" showed that he "intended other people would be able to access his stored child pornography and download it if they so desired." *Ibid.* The district court also relied on CPS software's report that child pornography files were available for download from Hayes's IP address. J.A. 530, 678. Neither basis is sufficient to include that Hayes intended to distribute child pornography. Therefore, there is not substantial evidence to support the Hayes's attempted distribution conviction and it must be reversed.

C. Merely making child pornography available for download over the Internet is not sufficient to support a conviction for distribution of child pornography.

Neither Pritchard nor any other investigator actually downloaded any child pornography from Hayes's IP address. J.A. 148. When Pritchard tried to connect to that address, he could not. J.A. 149. Nor did the Government present any evidence from others who downloaded child pornography from Hayes's IP address. The only evidence that any such files were ever available for download was the CPS report. As argued above, the CPS report should not have been admitted into evidence as it violated Hayes's right to confront witnesses against

him.[18] In addition, the information in the CPS report is inherently unreliable, to the extent it was never corroborated by investigators. Because none of the files allegedly offered for download were actually downloaded, it is impossible to accurately assess their content. As expert testimony explained, it is often necessary to view the content of a file once it has been downloaded to see if it matches the description provided in the file name. J.A. 357. The uncorroborated assertion that Hayes was making child pornography files available for download is not sufficient to sustain a conviction for attempting to distribute child pornography.

The only other evidence that suggested Hayes might have tried to distribute child pornography comes from his use of peer-to-peer file sharing software. Hayes had both FrostWire and Torrent file sharing programs on his computer when it was seized. J.A. 237, 357-358. FrostWire is a program in which the file sharing feature must be specifically enabled by the user for others across the Internet to have access to that user's shared files. J.A. 616-620. Both parties' experts agreed that, at some point in the past, the sharing feature had been enabled on Hayes's version of FrostWire. J.A. 229, 421-422. However, at the time of the search, that feature had been turned off. J.A. 338-339. Furthermore, because Hayes had a cache of non-pornographic material on his computer (movies, music, television shows) it is impossible to know if those were the files

[18] See pages 30 to 39.

he was sharing in the past, given that investigators failed to download any alleged child pornography from his IP address. J.A. 359, 385.

The Third Circuit recently concluded that the mere fact that a defendant has peer-to-peer software on his computer with file sharing enabled is not sufficient evidence to sustain a conviction for distribution of child pornography. *United States v. Husmann*, 765 F.3d 169 (3rd Cir. 2014). Placing certain files in a shared folder, the court noted, "does not automatically transmit them to another computer; shared files do not leave a user's computer until another program user actually downloads them." *Id.* at 171. Investigators "could not identify when these files were loaded to the shared file" or "if the files were ever downloaded to another machine." *Ibid* (internal quotation marks removed). Accordingly, the Government, as in this case, "did not present evidence that any person had actually downloaded or obtained the materials that Husmann made available." *Id.* at 170.

As a result, the court was forced to determine the definition of "distribution" under §2252(a)(2). *Husmann*, 765 F.3d at 172. Looking to the whole of the child pornography statutes enacted by Congress, the court concluded that because it had "separately criminalized offering, promoting, and attempting to distribute child pornography, a broad definition of the term 'distribute' would create unnecessary surplussage." *Id.* at 174. As a result, to "give effect to the entire statutory scheme, 'distribute' must require the transfer of possession of

child pornography to another person." *Ibid.* In doing so, the court rejected the Government's argument that the broader reading of distribution used in the United States Sentencing Guidelines should apply. *Id.* at 175-176, citing *United States v. Ramos*, 695 F.3d 1035, 1044 (10th Cir. 2012)("the statutory term has a distinct meaning and is not as broad as the same term under" the Guidelines).[19] Therefore, because "distribution requires a download or transfer of materials and the government did not present evidence" of such conduct, Husmann should not have been convicted. *Id.* at 176.

Although *Husmann* was decided after Hayes was sentenced, the district court applied the same logic by not convicting him of distribution of child pornography where "there's simply insufficient evidence to show that a transfer actually took place." J.A. 531. The district court erred by finding Hayes guilty of attempted distribution, however. The teaching of *Husmann* applies equally to that offense.

D. Nor is it sufficient to prove attempt to do so.

This Court has set out four elements that the government must prove to "establish that a defendant committed the crime of attempt." *United States v. Pratt*, 351 F.3d 131, 135 (4th Cir. 2003). First, it must prove that "the defendant had the requisite intent to commit a crime." *Ibid.* Second, it must prove the defendant

[19] This Court has held that merely making files available for download using peer-to-peer software triggers the Guideline enhancement. *United States v. Layton*, 564 F.3d 330, 335 (4th Cir. 2009).

"defendant undertook a direct act in a course of conduct planned to culminate in his commission of the crime." *Ibid.* Third, it must prove that act "was substantial, in that it was strongly corroborative of the defendant's criminal purpose." *Ibid.* Finally, it must prove that act "fell short of the commission of the intended crime due to intervening circumstances." *Ibid.* The Government failed to prove at least the first three of those elements beyond a reasonable doubt.

The Government failed to prove the first element because, under *Husmann* (and the district court's own reasoning), merely making files available over a peer-to-peer network is not the crime of distribution. Therefore, it cannot manifest the intent to commit the offense. The Government failed to prove the second element for the same reason. Taking actions that are not criminal cannot be part of a "course of conduct planned to culminate in his commission of the crime." Similarly, taking actions that are not a crime cannot be "strongly corroborative of the defendant's criminal purpose" if the end result of the defendant's actions is not criminal. Without those elements, the Government did not carry its burden of proving that Hayes committed an attempt offense. Notably, the district court did not reference any of the elements when concluding that Hayes was guilty of attempted distribution of child pornography. J.A. 524-531, 677-680.

IV. The imposition of a 15-year mandatory minimum sentence on Hayes based on the existence of prior convictions that were not charged in the indictment violated his Sixth Amendment rights.

A. Standard of Review

This Court reviews claims that a defendant's sentence violates the Sixth Amendment because certain facts were not presented to the grand jury *de novo*. See, *United States v. Mackins*, 315 F.3d 399, 405 (4th Cir. 2003).

B. A statute that requires an increased sentence based on the existence of a prior conviction that was not alleged in the indictment violates the Sixth Amendment.

All elements of an offense "must be charged in the indictment, submitted to a jury, and proven by the Government beyond a reasonable doubt." *Jones v. United States*, 526 U.S. 227, 232 (1999). As a result, "any fact that increases the penalty for a crime beyond the prescribed statutory maximum must be submitted to a jury, and proved beyond a reasonable doubt." *Apprendi v. New Jersey*, 530 U.S. 466, 490 (2000). That directive applies equally to facts that increase the mandatory minimum sentence for an offense. *Alleyne v. United States*, ___ U.S. ___, 133 S.Ct. 2151 (2013).

That rule is generally stated with a caveat – that it applies to any fact "[o]ther than the fact of a prior conviction." *Apprendi*, 530 U.S. at 466; *United States v. Booker*, 543 U.S. 220, 244 (2005). That caveat is a vestigial remnant of the Supreme Court's decision in *Almendarez-Torres v. United States*, 523 U.S. 224 (1998).

In *Almendarez-Torres*, the defendant pleaded guilty to illegally reentering the country after having been deported, in violation of 8 U.S.C. §1326(a), which provides a statutory maximum penalty of two years. However, §1326(b) increases the statutory maximum for those convicted of illegal reentry after having been deported following the commission of certain offenses. The indictment in *Almendarez-Torres* contained no allegation of the defendant's prior criminal history. Therefore, Almendarez-Torres argued that he could not be sentenced pursuant to any of the enhanced penalties found in §1326(b). *Almendarez-Torres*, 523 U.S. at 226-228.

A sharply divided Court rejected Almendarez-Torres's argument, with Justices Breyer, O'Connor, Kennedy and Thomas joining Chief Justice Rehnquist in that holding, stressing the history of recidivism as a sentencing factor, rather than an offense element. *Almendarez-Torres*, 523 U.S. at 230. Underlying the majority's opinion was a historical analysis showing that recidivism "is a traditional, if not the most traditional, basis for a sentencing court's increasing an offender's sentence," *id.* at 243, and to hold for Almendarez-Torres would "mark an abrupt departure from a longstanding tradition." *Id.* at 244. In a strong dissent, Justice Scalia, joined by Justices Stevens, Souter, and Ginsburg, refuted the majority's position as to the "tradition" of recidivism and concluded that "there is no rational basis for making recidivism an exception" to the protections of the Sixth Amendment. *Id.* at 258.

It was not long before *Almendarez-Torres* came under attack in *Apprendi*. Justice Stevens, writing for the five-member majority, wrote that *Almendarez-Torres* "represents at best an exceptional departure from the historic practice that we have described." *Apprendi*, 530 U.S. at 487. The majority conceded that "it is arguable that *Almendarez-Torres* was incorrectly decided, and that a logical application of our reasoning today should apply if the recidivist issue were contested." *Id.* at 489-490. Nevertheless, the Court declined to reach that issue because it was not raised by Apprendi and was not critical to the outcome of the case. *Id.* at 490.

Justice Thomas, one of the five members of the *Almendarez-Torres* majority, wrote a lengthy concurrence in *Apprendi* (joined by Justice Scalia) that effectively undermined the historical argument that recidivism should be an exception to the general *Apprendi* rule. *Apprendi*, 530 U.S. at 501-521. What was implicit in that concurrence has since become explicit, with Justice Thomas conceding, "*Almendarez-Torres* . . . has been eroded by this Court's subsequent Sixth Amendment jurisprudence, and a majority of this Court now recognizes that *Almendarez-Torres* was wrongly decided." *Shepard v. United States*, 544 U.S. 13, 27 (Thomas, J., concurring)(2005); see also, *Alleyne*, 133 S.Ct. at 2160, fn. 1 (specifically noting the *Almendarez-Torres* exception, but explaining that "[b]ecause the parties do not contest that decision's vitality, we do not revisit it for purposes of our decision today").

The statutory sentencing ranges on both of Hayes's convictions were increased based on his prior convictions. The range on the possession count increased from zero to 10 years in prison up to 10 to 20 years in prison. 18 U.S.C. §2252A(b)(2). On the attempted distribution count, the range increased from 5 to 20 years in prison up to 15 to 40 years in prison. 18 U.S.C. §2252A(b)(1). Hayes's sentence was increased by the finding of a fact not charged in the indictment. Under modern Sixth Amendment jurisprudence that should end the inquiry – Hayes's sentence should be vacated. Only the exception of *Almendarez-Torres*, which continues to cling to life, prevents that result. Because *Almendarez-Torres* is inconsistent with modern Sixth Amendment jurisprudence and recognized as such, it should be overruled.

CONCLUSION

For the reasons stated above, Hayes's conviction for attempted distribution of child pornography must be reversed and his case remanded to the district court for further proceedings. First, the district court erred by finding that Hayes had not laid a sufficient factual basis for entering a guilty plea to the charge of possession of child pornography. That error led to the Government's filing of a superseding indictment and Hayes being convicted both of possession and attempted distribution of child pornography. Second, the admission of the CPS records at trial, upon which the district court relied to find Hayes guilty of attempted distribution, was error in that it denied Hayes his right to confront the

witnesses against him. Finally, the Government did not produce sufficient evidence to prove, beyond a reasonable doubt, that Hayes had attempted to distribute child pornography.

REQUEST FOR ORAL ARGUMENT

Pursuant to Rule 34(a) of the Federal Rules of Appellate Procedure, Hayes requests oral argument. To counsel's knowledge, no cases presenting the first three issues have been decided by this Court. Given the lengthy record in this case, the nature of those issues, and the impact this Court's decision will have on child pornography prosecutions in the future, oral argument will aid the Court by providing it with the most developed basis for making its decision.

Respectfully submitted,

JOHN D. HAYES

By Counsel

BRIAN J. KORNBRATH
ACTING FEDERAL PUBLIC DEFENDER

s/Jonathan D. Byrne
Jonathan D. Byrne
Appellate Counsel
Office of the Federal Public Defender
Room 3400, United States Courthouse
300 Virginia Street East
Charleston, West Virginia 25301
E-mail: jonathan_byrne@fd.org

s/David R. Bungard
David R. Bungard
Assistant Federal Public Defender
Office of the Federal Public Defender
Room 3400, US Courthouse
300 Virginia Street East
Charleston, West Virginia 25301
E-mail: david_bungard@fd.org

CERTIFICATE OF COMPLIANCE
WITH TYPEFACE AND LENGTH LIMITATIONS

1. This brief complies with the type-volume limitation of F.R.A.P. 28.1(e)(2) or F.R.A.P. 32(a)(7)(B) because this brief contains **12,189** words, excluding the parts of the brief exempted by F.R.A.P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of F.R.A.P. 32(a)(5) and the type style requirements of F.R.A.P. 32(a)(6) because this brief has been prepared using Microsoft Word 2010 in 14 point Garamond.

DATE: November 5, 2014

s/Jonathan D. Byrne
Jonathan D. Byrne
Appellate Counsel
Room 3400, United States Courthouse
300 Virginia Street East
Charleston, West Virginia 25301
E-mail: jonathan_byrne@fd.org

s/David R. Bungard
David R. Bungard
Assistant Federal Public Defender
Room 3400, United States Courthouse
300 Virginia Street East
Charleston, West Virginia 25301
E-mail: david_bungard@fd.org

CERTIFICATE OF SERVICE

We hereby certify that on **November 5, 2014** the foregoing **BRIEF** was electronically filed with the Clerk of Court using the CM/ECF System, which will send notice of such filing to the following registered CM/ECF user:

Jennifer Rada Herrald
Assistant United States Attorney
United States Courthouse, Room 4000
300 Virginia Street East
Charleston, West Virginia 25301
Email: jennifer.herrald@usdoj.gov

and served upon the Appellant by United States Mail, first class postage prepaid, addressed as follows:

Mr. John D. Hayes
South Central Regional Jail
1001 Centre Way
Charleston, WV 25309

s/Jonathan D. Byrne
Jonathan D. Byrne
Appellate Counsel
Room 3400, United States Courthouse
300 Virginia Street East
Charleston, West Virginia 25301
E-mail: jonathan_byrne@fd.org

s/David R. Bungard
David R. Bungard
Assistant Federal Public Defender
Room 3400, United States Courthouse
300 Virginia Street East
Charleston, West Virginia 25301
E-mail: david_bungard@fd.org